

# (12) UK Patent Application (19) GB (11) 2 357 225 (13) A

(43) Date of A Publication 13.08.2001

(21) Application No 9929029.8

(22) Date of Filing 08.12.1999

(71) Applicant(s)  
Hewlett-Packard Company  
(Incorporated in USA - Delaware)  
3000 Hanover Street, Palo Alto, California 94304,  
United States of America

(72) Inventor(s)  
Michael John Wray

(74) Agent and/or Address for Service  
Robert Francis Squibbs  
Hewlett-Packard Limited, Intellectual Property  
Section, Building 2, Filton Road, Stoke Gifford,  
BRISTOL, BS12 6QZ, United Kingdom

(51) INT CL<sup>7</sup>  
H04L 9/32

(52) UK CL (Edition S )  
H4P PDCSA

(56) Documents Cited  
EP 0586022 A1 EP 0503765 A2 WO 96/02993 A2

(58) Field of Search  
UK CL (Edition R ) G4A AAP , H4P PDCSA  
INT CL<sup>7</sup> G06F 1/00 , H04L 9/32  
Online: EPODOC, JAPIO, WPI

(54) Abstract Title  
Electronic certificate with validity subject to external conditions

(57) An electronic or digital certificate has content data specifying an attribute delegation, some benefit or right conferred by the certificate, from an identified issuer to the subject of the certificate. The content data also specifies a condition (40) that must be met for the delegation to be valid. The certificate may identify the subject who is delegated the attribute by the certificate or any subject which satisfies the condition may be delegated the attribute. The condition requires that a particular subject must have a particular attribute in order to meet the criteria for the condition, this particular subject may or may not be the same as the subject of the certificate.

The condition may specify multiple attributes that the particular subject must have which may be combined in a logical relationship.

The certificate also includes an electronic or digital signature confirming its contents and may be an SPKI certificate.

Reduction and trust chain discovery engines for use with the certificates are also disclosed.

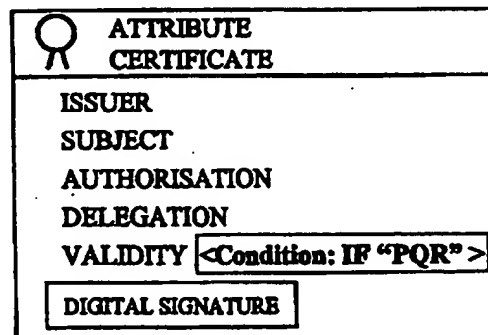
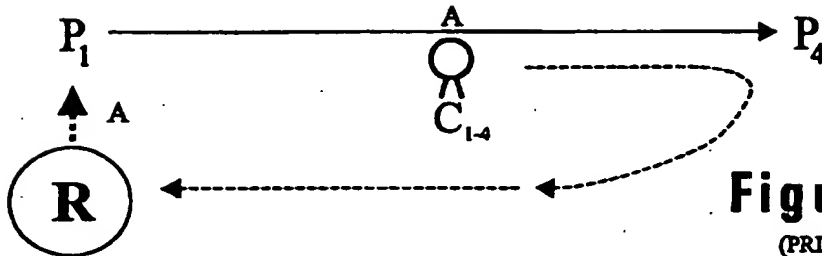


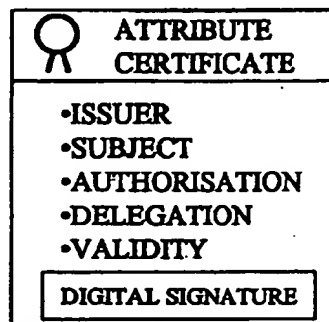
Figure 5

GB 2 357 225 A

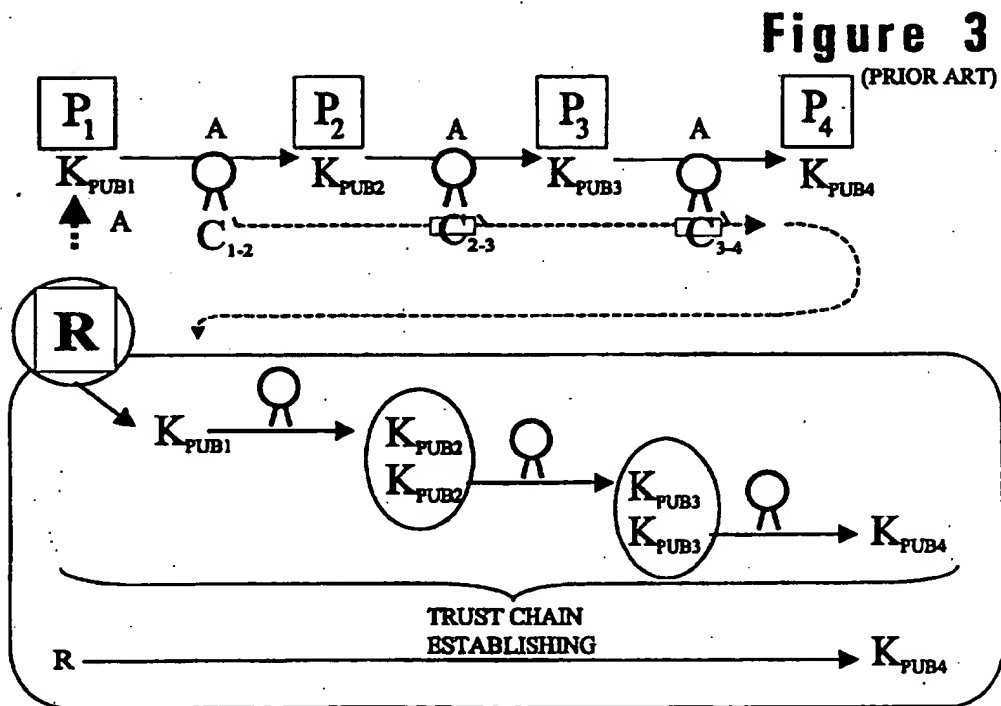
1/8



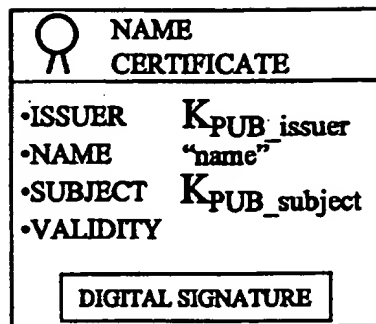
**Figure 1**  
(PRIOR ART)



**Figure 2**  
(PRIOR ART)

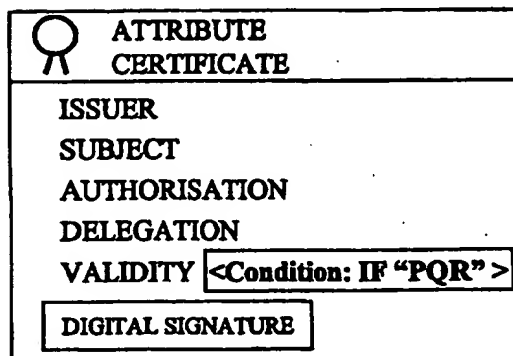


2/8



**Figure 4**  
(PRIOR ART)

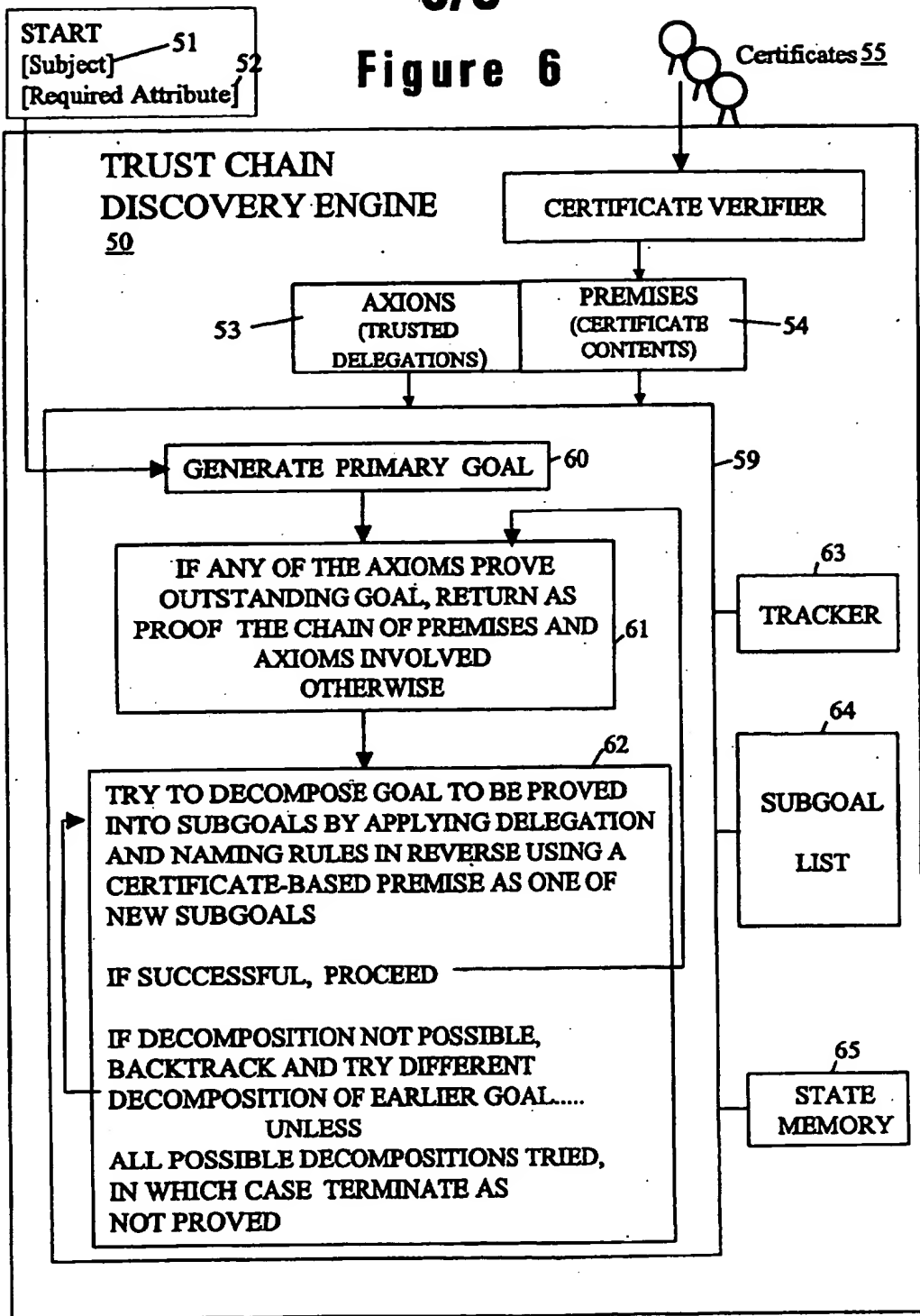
$$K_{\text{PUB\_issuer}} \cdot \text{"name"} = K_{\text{PUB\_subject}}$$

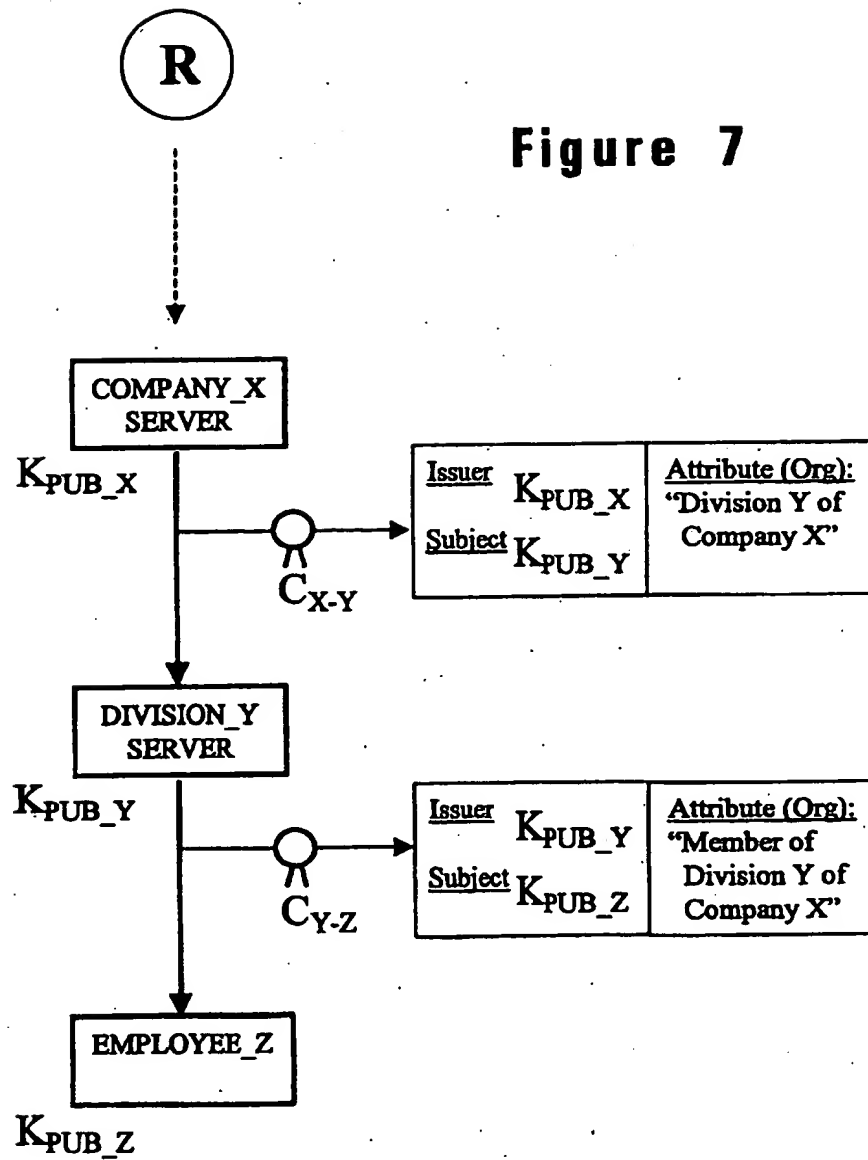


**Figure 5**

3/8

Figure 6





5/8

RESOURCE REQUIRES:	REQUESTOR IS MEMBER OF ACCREDITED ORGANISATION
PREMISES	$C_{X-Y}$ $K_{PUB\_X} \xrightarrow{\text{"Division Y of Company X"}} K_{PUB\_Y}$ $C_{Y-Z}$ $K_{PUB\_Y} \xrightarrow{\text{"Member of Division Y of Company X"}} K_{PUB\_Z}$
RELEVANT AXIOM	SELF $\xrightarrow{\text{Company X}} K_{PUB\_X}$
PRIMARY GOAL	<pre> graph TD     G1["&lt;SELF -&gt; K_PUB_Z&gt;"]     G2["&lt;SELF -&gt; K_PUB_Y&gt;"]     G3["&lt;K_PUB_Y -&gt; K_PUB_Z&gt;"]     G4["&lt;SELF -&gt; K_PUB_X&gt;"]     G5["&lt;K_PUB_X -&gt; K_PUB_Y&gt;"]     G1 --&gt; G2     G1 --&gt; G3     G3 --- J1["JUSTIFIED BY C_Y-Z"]     G2 --&gt; G4     G2 --&gt; G5     G4 --- J2["JUSTIFIED BY AXIOM"]     G5 --- J3["JUSTIFIED BY C_X-Y"] </pre>
FIRST DECOMPOSITION	
SECOND DECOMPOSITION	

Figure 8

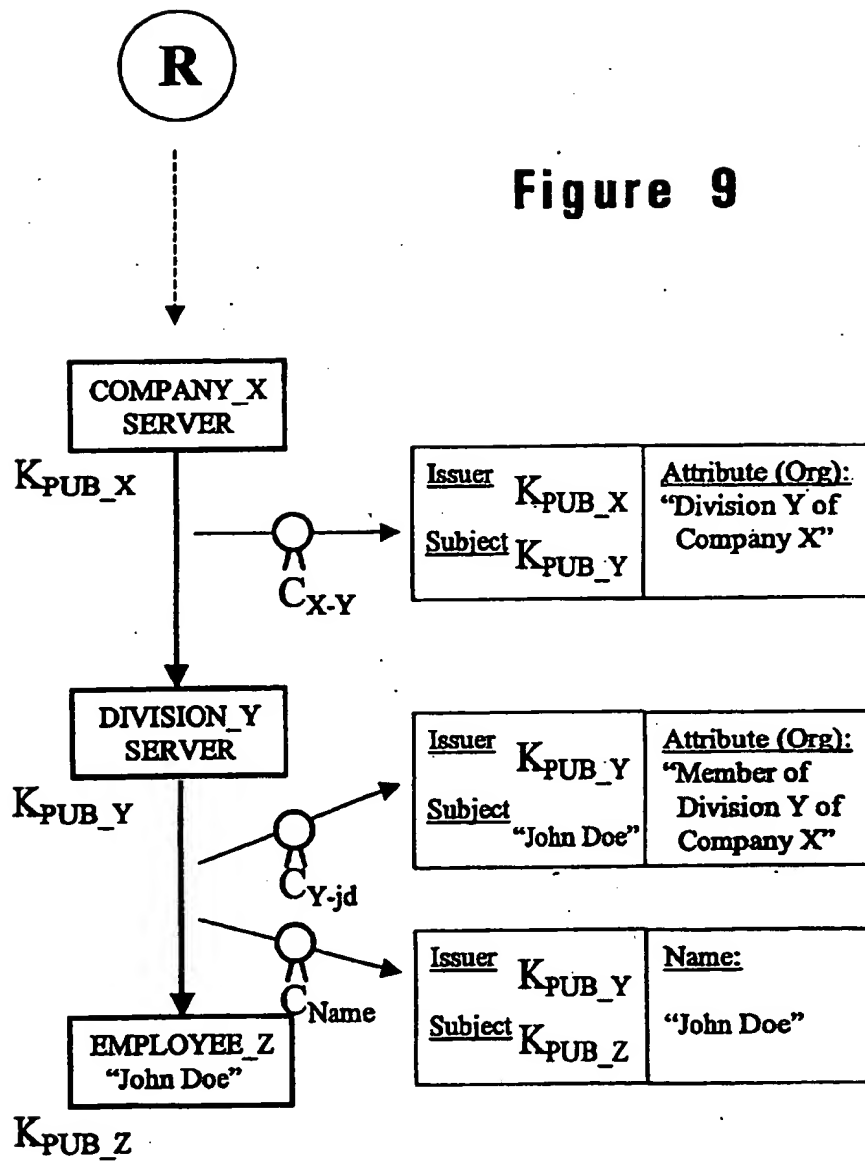


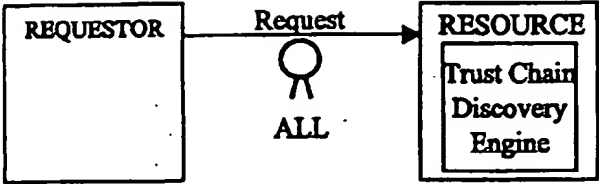
Figure 9

RESOURCE REQUIRES:	REQUESTOR IS MEMBER OF ACCREDITED ORGANISATION
PREMISES	$C_{X-Y} \quad K_{PUB\_X} \xrightarrow{\text{"Division Y of Company X"}} K_{PUB\_Y}$ $C_{Y-jd} \quad K_{PUB\_Y} \xrightarrow{\text{"Member of Division Y of Company X"}} \text{"John Doe"}$ $C_{Name} \quad K_{PUB\_Y} \cdot [\text{"John Doe"}] = K_{PUB\_Z}$
RELEVANT AXIOM	$SELF \xrightarrow{\text{Company X}} K_{PUB\_X}$
PRIMARY GOAL	$\langle SELF \rightarrow K_{PUB\_Z} \rangle$
FIRST DECOMPOSITION	$\langle SELF \rightarrow \text{"John Doe"} \rangle \times \langle \text{"John Doe"} \rightarrow K_{PUB\_Z} \rangle$ <div style="border: 1px solid black; padding: 2px; width: fit-content; margin-left: auto; margin-right: auto;">JUSTIFIED BY <math>C_{Name}</math></div>
SECOND DECOMPOSITION	$\langle SELF \rightarrow K_{PUB\_Y} \rangle \quad \langle K_{PUB\_Y} \rightarrow \text{"John Doe"} \rangle$ <div style="border: 1px solid black; padding: 2px; width: fit-content; margin-left: auto; margin-right: auto;">JUSTIFIED BY <math>C_{Y-jd}</math></div>
THIRD DECOMPOSITION	$\langle SELF \rightarrow K_{PUB\_X} \rangle \quad \langle K_{PUB\_X} \rightarrow K_{PUB\_Y} \rangle$ <div style="display: flex; justify-content: space-around; margin-top: 10px;"> <div style="border: 1px solid black; padding: 2px; text-align: center;">JUSTIFIED BY AXIOM</div> <div style="border: 1px solid black; padding: 2px; text-align: center;">JUSTIFIED BY <math>C_{X-Y}</math></div> </div>

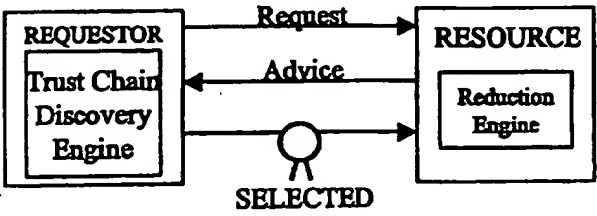
Figure 10



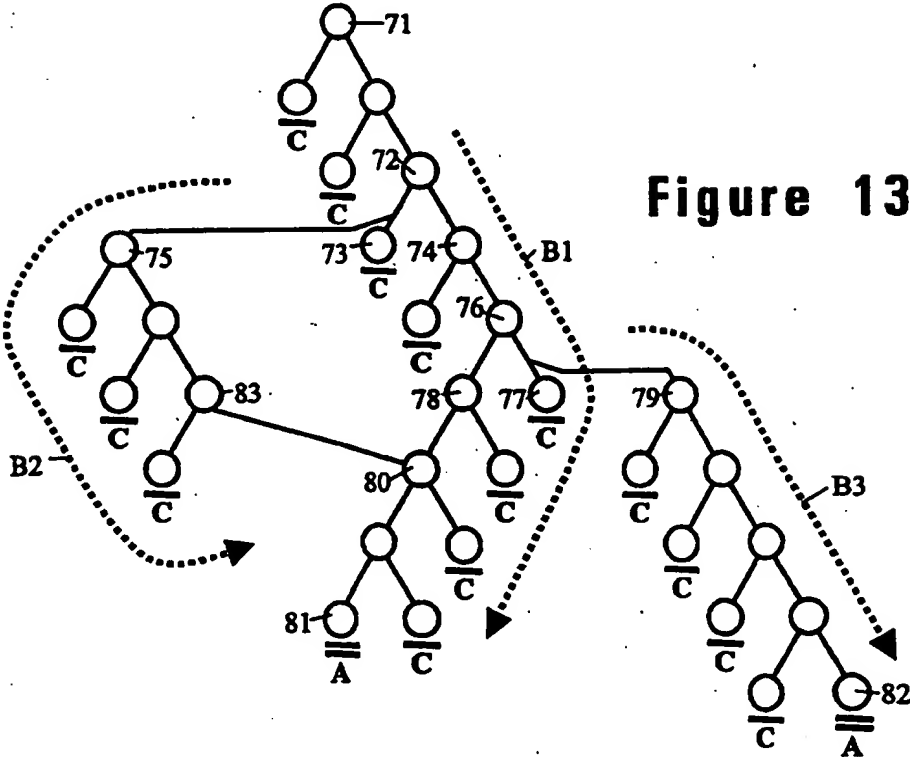
8/8



## Figure 11



## Figure 12



## Figure 13